



UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office

Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.
09/328,726	10/26/98	COLLINS	T 2026-25 (PT-T)

LEAH SHERRY
OPPENHEIMER, WOLFF & DONNELLY, LLP
1400 PAGE MILL ROAD
PALO ALTO CA 94304

TM02/0402

EXAMINER

LEANTING T	ART UNIT	PAPER NUMBER
------------	----------	--------------

2131
DATE MAILED:
04/02/01

19
(Handwritten signature)

Please find below and/or attached an Office communication concerning this application or proceeding.

Commissioner of Patents and Trademarks

1- File Copy

Office Action Summary

	Application No.	Applicant(s)
	09/328,726	COLLINS ET AL.
Examiner	Art Unit	
Jeffrey Scott Leaning	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

Extensions of time may be available under the provisions of 37 CFR 1.136 (a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.

- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on 31 January 2001.
2a) This action is FINAL. 2b) This action is non-final.
3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 14-92 is/are pending in the application.
4a) Of the above claim(s) _____ is/are withdrawn from consideration.
5) Claim(s) _____ is/are allowed.
6) Claim(s) 14-92 is/are rejected.
7) Claim(s) _____ is/are objected to.
8) Claims _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
10) The drawing(s) filed on _____ is/are objected to by the Examiner.
11) The proposed drawing correction filed on _____ is: a) approved b) disapproved.
12) The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. § 119

- 13) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) All b) Some * c) None of:
1. Certified copies of the priority documents have been received.
2. Certified copies of the priority documents have been received in Application No. _____.
3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
* See the attached detailed Office action for a list of the certified copies not received.
14) Acknowledgement is made of a claim for domestic priority under 35 U.S.C. § 119(e).

Attachment(s)

- 15) Notice of References Cited (PTO-892)
16) Notice of Draftsperson's Patent Drawing Review (PTO-948)
17) Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____.

- 18) Interview Summary (PTO-413) Paper No(s) _____.
19) Notice of Informal Patent Application (PTO-152)
20) Other:

Art Unit: 2131

DETAILED ACTION

1. Claims 14-92 are pending in the present application. Claims 14-92 stand rejected.
2. Due to the notation-intensive nature of the application, the examiner will state the conventions that he will use. Underscore marks will denote subscripts, so "a sub" will be denoted by "a_b". Carets will denote superscripts, so "a to the b" will be denoted by "a^b".

Claim Rejections - 35 USC § 112

3. The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.
4. Claims 14-46 are rejected under 35 U.S.C. 112, first paragraph, as containing subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention. See the enumerated items below.
5. Claims 14-46 are also rejected under 35 U.S.C. 112, first paragraph, as containing subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. The applicant is required to either cancel the claims as referring to new matter or address their support.

Application/Control Number: 09/328,726

Art Unit: 2131

a. Claims 14, 15, 16, 22, 27, 32, 37, and 42 as amended, include the provision of being “backwards compatible with preexisting public key infrastructure”. The examiner requests that the applicant point out where in the specification the term “backwards compatible” appears, or , barring that, where in the specification support appears for this expedient. As it stands, the specification does not support this term nor even disclose it.

b. Claims 14 and 15 recite that the processing involves a “minimal amount of computer instructions”. This term is not disclosed by the applicant, nor is it enabled by the specification. The examiner requests that the applicant point out where in the specification the term “minimal amount of computer instructions” appears, or , barring that, where in the specification support appears for this expedient.

c. Claims not specifically addressed are rejected by virtue of their dependence on rejected claims.

6. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

7. Claims 14 and 15 rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

a. These claims recite a “minimal amount of computer instructions”. The scope of this term is unclear for the following reasons. The term “minimal” is uncertain because the

Art Unit: 2131

measured quantity to which it refers may be, for just some examples, the number of symbols in the programming language, the number of memory cells required to store it, the number of processing steps required, the amount of time required, the compilation time required, and so on. For the purposes of this action, the examiner interprets this term to mean that the algorithm is somehow efficient or fast.

Claim Rejections - 35 USC § 102

8. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless --

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

9. Claims 14-66 rejected under 35 U.S.C. 102(b) as being anticipated by Rivest *et al* (US 4,405,829).
- a. Claim 14 is directed to an RSA type system including encryption and decryption. Rivest *et al* disclose this system, see the summary of the invention starting on line 12 of column 4. Additionally, the applicant's invention is particularly directed to the following two features: (1) using more than two primes in the modulus, and (2) using the Chinese Remainder Theorem to speed up decryption. Rivest *et al* also discloses both of those features, see column 13 lines 29-34. The particular equations specified in claim 14 lines 11-24 and 30-32, and in the corresponding

Art Unit: 2131

parts of the other claims, are inherent in using the Chinese Remainder Theorem for decoding as taught by Rivest *et al.*

b. Claim 15 is similar to claim 14 except the message is decrypted using the

corresponding formulae and steps. See the above.

c. Claim 16 is a system embodiment which includes the encoding of claim 14 and the

decoding of claim 15 and is rejected on analogous grounds as being obvious as such.

d. Claims 17-21 are system claims for encoding and decoding a message and are

therefore rejected on grounds analogous to those used to reject claims 14, 15, and 16.

e. Claims 22-26 are system claims for encoding and decoding a message and are

therefore rejected on grounds analogous to those used to reject claims 14, 15, and 16.

f. Claims 27-31 are method claims for encoding a message and are therefore rejected

on grounds analogous to those used to reject claim 14.

g. Claims 32-36 are system claims for encoding a message and are therefore rejected

on grounds analogous to those used to reject claim 14.

h. Claims 37-41 are method claims for decoding a message and are therefore rejected

on grounds analogous to those used to reject claim 15.

i. Claims 42-46 are system claims for decoding a message and are therefore rejected

on grounds analogous to those used to reject claim 16.

Art Unit: 2131

j. Rivest *et al* also disclose that their invention can digitally sign and verify digital signatures, see column 4 lines 1-6, and the summary of using their invention in that capacity starting at column 5 line 18.

i. Claims 47-51 are method claims for signing a message and are rejected on grounds analogous to those used to reject claims 14 and 15 and further in light of paragraph j above.

ii. Claims 52-56 are system claims for signing a message and are rejected on grounds analogous to those used to reject claims 14, 15, and 16 and further in light of paragraph j above.

iii. Claims 57-61 are procedure claims for signing a message and are rejected on grounds analogous to those used to reject claims 14, 15, and 16 and further in light of paragraph j above.

iv. Claims 62-66 are system claims for signing a message and are rejected on grounds analogous to those used to reject claims 14, 15, and 16 and further in light of paragraph j above.

Claim Rejections - 35 USC § 103

10. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are

Art Unit: 2131

such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

11. Claims 67-92 rejected under 35 U.S.C. 103(a) as being unpatentable over Rivest *et al* as applied above, and further in view of Menezes *et al*. Claims 67-92 are dependent claims which are directed to two features. The examiner addresses them here.

a. Claims 67 *et al* are directed to processing the sub-tasks by way of a plurality of exponentiation units operating substantially independently. Menezes *et al* discloses simultaneous multiple exponentiation, see Note 14.87(iii) on page 617. It would be obvious to one of ordinary skill in the art to use this method in the invention of Rivest *et al* because of Menezes *et al*'s suggestion that efficient exponentiation is essential to employing the RSA algorithm, see the first two paragraphs of Section 14.6 Exponentiation on page 613.

b. Claims 68 *et al* are directed to insuring that each of the random primes has the same number of bits. Menezes *et al* discloses that each of the primes used should be "roughly the same size". It would be obvious to one of ordinary skill in the art to ensure that the number of bits for each of the primes is the same size in the invention of Rivest *et al* because of Menezes *et al*'s suggestion that they should be roughly the same size. Note that "roughly the same size" discloses a range which includes identity.

12. Claims 14-92 rejected under 35 U.S.C. 103(a) as being unpatentable over Menezes *et al* in view of Quisquater *et al*.

Art Unit: 2131

a. Claim 14 is directed to a method for establishing cryptographic communications.

Menezes *et al* teach of a computation method for processing secret information, see section 8.2 (pp. 285-291).

i. Both Section 8.2 of Menezes *et al* and the applicants use RSA-type

cryptography. This cryptography employs a modulus consisting of a product of prime numbers. In the case of Section 8.2, there are two numbers in the modulus and they are called 'p' and 'q'. In the cases of the applicants there are possibly more than two prime numbers in the modulus and they are called p_1, p_2, \dots, p_n . Hence, p corresponds to p_1 , and q corresponds to p_2 . This is merely notation, and the examiner point it out for the sake of clarity. The essential features are identical.

ii. Menezes *et al* teach of encoding a plaintext word M to a ciphertext word

C, see Algorithm 8.3. Menezes *et al* disclose that M is of a certain size, less than a fixed size, see Message Blocking on page 285. It is inherent that the message block size for RSA (the method of section 8.2) is $n-1$ where n is the product of prime integers.

iii. Menezes *et al* teach of transforming ciphertext C to message M, see

Algorithm 8.3. Note that a corresponding decryption is also disclosed.

iv. The number 'e' is selected as being relatively prime to the described lcm

(least common multiple), see Algorithm 8.1 and Note 8.5.

Art Unit: 2131

v. Section 8.2 of Menezes *et al* lacks a teaching that there can be more than two primes in the modulus, that the quantities of lines 10-24 of claim 14 are computed, that the data is (re)combined (as in lines 28-32 of claim 14), and that the system is backwards compatible.

(1) Menezes *et al* teach that the RSA encryption problem relies on the difficulty of the integer factorization problem, see the introduction to section 3.2. Menezes *et al* further teach that the integer factorization problem comes from factoring the product of multiple primes $p_1^{e1} p_2^{e2} \dots p_k^{ek}$, see definition 3.3. The security of the RSA system (Section 8.2) is in fact equivalent to the integer factorization problem, see section 8.2.2(I) and Fact 8.6. It would be obvious for one of ordinary skill in the art to modify the system of Section 8.2 to have a modulus having the number of primes, 'k', being a number greater than 2 because the difficulty of the integer factorization problem provides the security for the cryptosystem. Note that with this combination, we now have a cryptosystem with multiple primes, hence we no longer have just p and q but rather p_1, p_2, \dots, p_k . This is relevant in interpreting the next two paragraphs.

(2) Quisquater *et al* disclose that the quantities of lines 10-24 are computed, see page 906 first column. It would be obvious to one of ordinary skill in the art to include these computations because of Quisquater *et al*'s clear suggestion to employ the Chinese Remainder Theorem into the computations involved with the RSA cryptosystem, see the title and the abstract on page 905. Note that Quisquater *et al*'s method is described as being "fast".

Art Unit: 2131

(3) In the interest of producing a complete and readable action which addresses each of the claims and which utilizes the information gained by the interview (see the examiner's interview summary), the examiner here addresses two algorithms by which obviousness of recombining the data are established. The subsequent claims are each directed to one of these two algorithms. The algorithms are Gauss' Algorithm which is detailed in (a), and Garner's Algorithm, which is detailed in (b).

(a) Menezes *et al* in Section 2.4.3 discloses that the quantities of lines 28-32 are computed, see Gauss' Algorithm (Algorithm 2.121). The following are some correspondences for the reader's convenience. The applicant's w_i is Menezes *et al*'s N_i . The applicant's n is Menezes *et al*'s n . The applicant's Y_i are Menezes *et al*'s partial sums of x , where Menezes *et al* disclose that x is a sum as in Algorithm 2.121 line 2. It would be obvious to one of ordinary skill in the art to employ this algorithm for solving the Chinese Remainder Theorem (CRT) problem which arises in RSA cryptography because of Quisquater *et al*'s explicit suggestion the CRT may be used to expedite the calculation of RSA (see Quisquater *et al*'s abstract) and because Menezes *et al* discloses Gauss' Algorithm may be used to solve the CRT, see Algorithm 1.121 itself. Note that The examiner accounts for the "recursive" aspect of claim 14 by noting that computers usually compute sums as in Algorithm 2.121 recursively, and takes official notice of such. It would be obvious to compute the quantities recursively because of the added speed and memory expediency conveyed by recursive computation.

Art Unit: 2131

(b) Menezes *et al* in Section 14.5.2 discloses that the CRT data may be combined (or computed), see Garner's Algorithm (Algorithm 14.5.2). The following are some correspondences for the reader's convenience. Note that Garner's algorithm is recursive. It would be obvious to one of ordinary skill in the art to employ this algorithm for solving the Chinese Remainder Theorem (CRT) problem which arises in RSA cryptography because of Quisquater *et al*'s explicit suggestion the CRT may be used to expedite the calculation of RSA (see Quisquater *et al*'s abstract) and because Menezes *et al* discloses Garner's Algorithm may be used to efficiently solve the CRT, see Algorithm 1.121 itself.

(4) That the well-known RSA cryptosystem is a special case of the above combination indicates that it is backwards compatible with RSA.

b. Claim 15 is similar to claim 14 except the message is decrypted using the corresponding formulae and steps. See the above.

c. Claim 16 is a system embodiment which includes the encoding of claim 14 and the decoding of claim 15 and is rejected on analogous grounds as being obvious as such.

d. Claims 17-21 are system claims for encoding and decoding a message and are therefore rejected on grounds analogous to those used to reject claims 14, 15, and 16.

e. Claims 22-26 are system claims for encoding and decoding a message and are therefore rejected on grounds analogous to those used to reject claims 14, 15, and 16.

f. Claims 27-31 are method claims for encoding a message and are therefore rejected on grounds analogous to those used to reject claim 14.

Art Unit: 2131

g. Claims 32-36 are system claims for encoding a message and are therefore rejected on grounds analogous to those used to reject claim 14.

h. Claims 37-41 are method claims for decoding a message and are therefore rejected on grounds analogous to those used to reject claim 15.

i. Claims 42-46 are system claims for decoding a message and are therefore rejected on grounds analogous to those used to reject claim 16.

j. The examiner takes as official notice that it is notoriously well-known to those of ordinary skill in the art to use RSA type cryptography for signing and verifying messages. It would be obvious to one of ordinary skill in the art to use RSA type cryptography to sign messages and verify such signatures because of the security and irrefutability available from such expedients.

i. Claims 47-51 are method claims for signing a message and are rejected on grounds analogous to those used to reject claims 14 and 15 and further in light of the above official notice.

ii. Claims 52-56 are system claims for signing a message and are rejected on grounds analogous to those used to reject claims 14, 15, and 16 and further in light of the above official notice.

iii. Claims 57-61 are procedure claims for signing a message and are rejected on grounds analogous to those used to reject claims 14, 15, and 16 and further in light of the above official notice.

Art Unit: 2131

iv. Claims 62-66 are system claims for signing a message and are rejected on grounds analogous to those used to reject claims 14, 15, and 16 and further in light of the above official notice.

k. Claims 67-92 are dependent claims which are directed to two features. The examiner addresses them here.

i. Claims 67 *et al* are directed to processing the sub-tasks by way of a plurality of exponentiation units operating substantially independently. Menezes *et al* discloses simultaneous multiple exponentiation, see Note 14.87(iii) on page 617. It would be obvious to one of ordinary skill in the art to use this method in the combination recited in the parent claims because of Menezes *et al*'s suggestion that efficient exponentiation is essential to employing the RSA algorithm, see the first two paragraphs of Section 14.6 Exponentiation on page 613.

ii. Claims 68 *et al* are directed to insuring that each of the random primes has the same number of bits. Menezes *et al* discloses that each of the primes used should be "roughly the same size". It would be obvious to one of ordinary skill in the art to ensure that the number of bits for each of the primes is the same because of Menezes *et al*'s suggestion that they should be roughly the same size. Note that "roughly the same size" discloses a range, which includes in the range the identity.

Art Unit: 2131

Response to Arguments

13. Applicant's arguments filed 31 January 2001 have been fully considered but they are not persuasive.

- a. The non statutory double patenting rejections have been removed in response to the applicant's terminal disclaimer.
- b. The applicant's remarks regarding the 35 USC 103 rejection are now moot in view of the new grounds for rejection.
- c. The following remarks are directed to the applicant's summary of the interview with the applicant.

Conclusion

14. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Rivest *et al* (US 4,405,829, see column 13 lines 29-34) and Slavin (US 5,974,151, see the abstract) disclose multi-prime (more than two) RSA systems.

15. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jeffrey Scott Leaning whose telephone number is (703) 306-5975. The examiner can normally be reached on weekdays from 9:00am to 5:00pm.

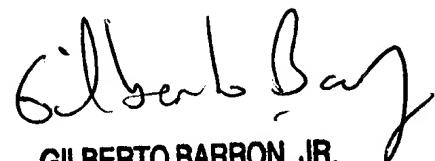
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gail Hayes, can be reached on (703) 305-9711. The fax phone number for the organization where this application or proceeding is assigned is (703) 308-9051.

Art Unit: 2131

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

Jeffrey Scott Leaning

27 March 2001



GILBERTO BARRON, JR.
PRIMARY EXAMINER
ART UNIT 2131